Fail2Ban

written by archi | 15 kwietnia 2021

Laboratorium ma na celu wprowadzenie mechanizmów bezpieczeństwa do systemów sieciowych. W tym przypadku zostanie uruchomione oprogramowanie przeznaczone do analizowaniu dzienników zdarzeń systemu i aplikacji na nim działających w celu prowadzenia polityki bezpieczeństwa. Ideą działania pakietu Fail2Ban jest aktywne wpływanie na system zapory ogniowej (firewall) poprzez blokowanie hostów atakujących lub prowadzących nie właściwe działania. Takie działania mogą wynikać np. z prób logowania się na obce konta.

1. Aktualizuj bazę dostępnego oprogramowania w systemie

```
apt-get update
```

2. Zainstaluj pakiet „fail2ban”

```
apt-get install fail2ban
```

3. W katalogu „`/etc/fail2ban`” zostały zgromadzone pliki konfiguracyjne tego pakietu.

```
fail2ban
├ /action.d
│    ├ abuseipdb.conf
│    │  [...]
│    └ -xarf-login-attack.conf
├ /fail2ban.d
├ /filter.d
│    ├ /ignorecommands
│    ├ 3proxy.conf
│    │  [...]
│    └ zoneminder.conf
```

```
├ /jail.d
│     └ defaults-debian.conf
├ fail2ban.conf
├ jail.conf
├ paths-arch.conf
├ paths-common.conf
├ paths-debian.conf
└ paths-opensuse.conf
```

4. Należy włączyć sprawdzanie dla „**sshd**„, „**webmin-auth**” w pliku „`/etc/fail2ban/jail.d/defaults-debian.conf`„

5. W pliku „`/etc/fail2ban/jail.conf`” należy zmienić wartości domyślne dla: bantime = 1m, findtime = 1m i maxretry = 3

```
# "bantime" is the number of seconds that a host is banned.
bantime  = 1m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 1m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5
```

W tym samym pliku podane są domyślnie parametry dla kolejnych włączonych wcześniej więzień (jail)

```
[sshd]

port    = ssh
logpath = %(sshd_log)s


[sshd-ddos]
# This jail corresponds to the standard configuration in Fail2ban.
# The mail-whois action send a notification e-mail with a whois request
# in the body.
port    = ssh
logpath = %(sshd_log)s
```

```
[webmin-auth]

port    = 10000
logpath = %(syslog_authpriv)s
```

6. Po wprowadzeniu wszystkich zmian restartujemy usługę:

```
services fail2ban restart
```

7. Sprawdzimy czy usługa działa poprawnie:

`fail2ban-client`

8. Wykonamy test sprawdzający czy więzienie dla Webmin-Auth działa:

– wykonaj polecenie dla sprawdzenia wpisów

```
fail2ban-client status
```

– w wyniku powinieneś zobaczyć odpowiedź systemu

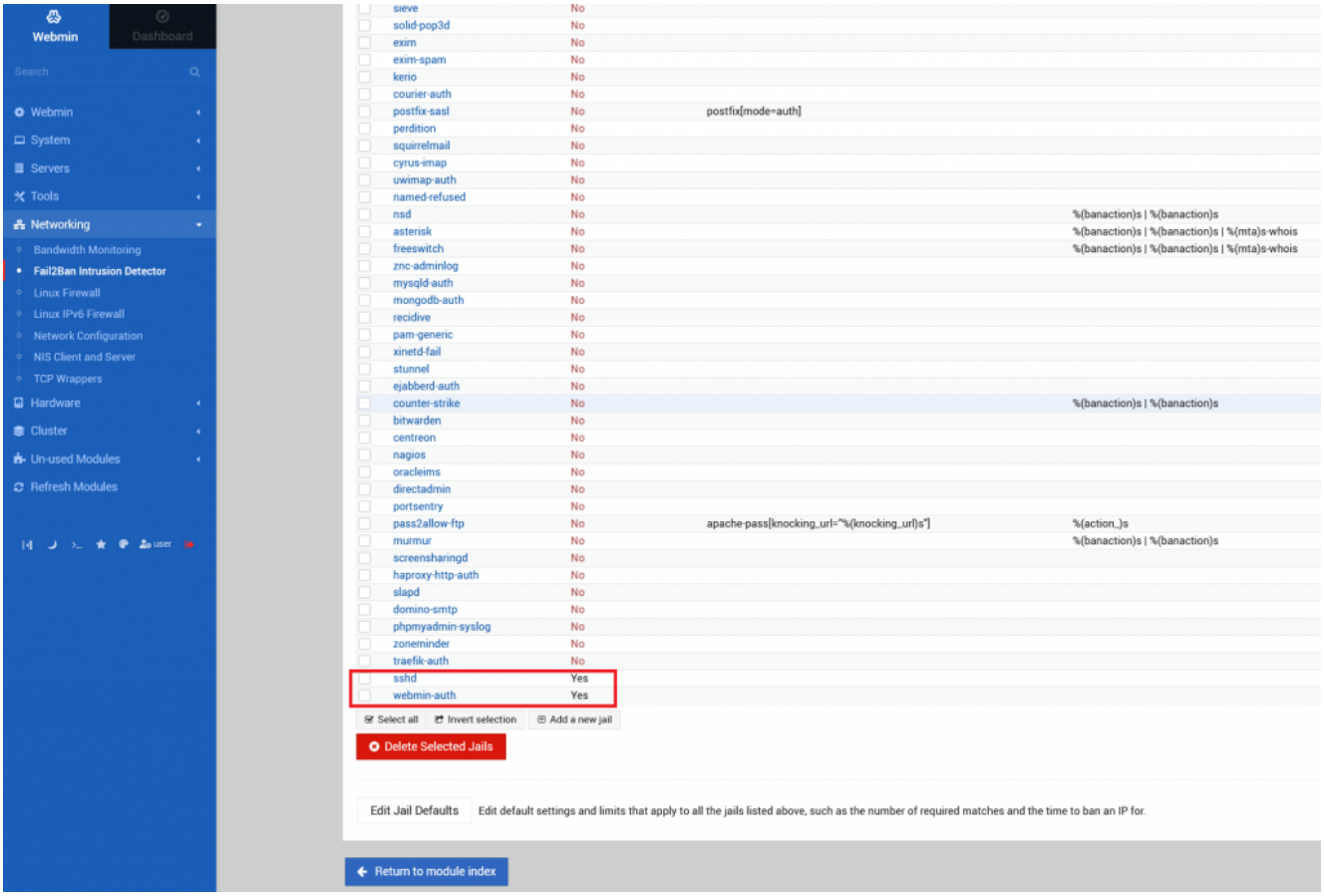
```
Status
|- Number of jail:      2
`- Jail list:   sshd, webmin-auth
```

– sprawdzimy wpisy w Firewall

```
iptables -L -n
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Sprawdzenie możesz również wykonać poprzez Webmin



– informacje w systemie pojawią się dopiero po wykonaniu lub pojawieniu się blokad po nieuprawnionych działaniach w systemie

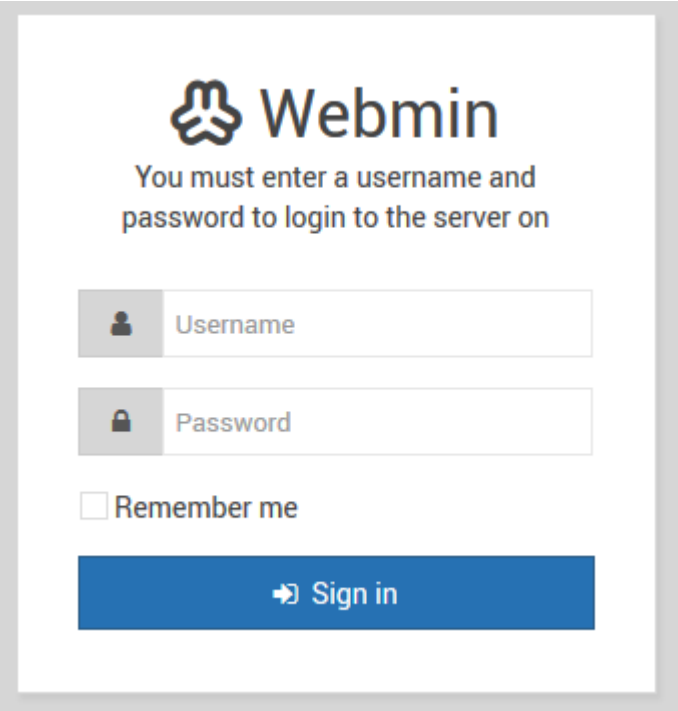
```
root@linux:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-webmin-auth  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 10000

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-webmin-auth (1 references)
target     prot opt source               destination
REJECT     all  --  192.168.99.129       0.0.0.0/0           reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

– zaloguj się na stronie „`https://192.168.x.x:10000/`” do konsoli Webmin w sposób prawidłowy oraz następnie wykonaj 3x błędne logowanie



– gdy zalogujemy się niepoprawnie po raz trzeci (3) to nastąpi zablokowanie dostępu dla adresu IP z którego się logowaliśmy i dostęp do strony Webmin będzie zablokowany na ustawiony wcześniej czas 60s.

```
Chain f2b-sshd-ddos (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain f2b-webmin-auth (1 references)
target     prot opt source               destination
REJECT     all  --  82.145.93.80         0.0.0.0/0           reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Jeśli uzyskasz taki efekt to usługa została skonfigurowana poprawnie...